UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/693,585	10/24/2003	Klaus U. Schutz	MS1-1819US	1086

22801 7590 10/17/2008

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
COLAN, GIOVANNA B	

ART UNIT	PAPER NUMBER
2162	

MAIL DATE	DELIVERY MODE
10/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/693,585	SCHUTZ ET AL.	
	Examiner	Art Unit	
	GIOVANNA COLAN	2162	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 August 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9 – 14, 17 – 23, and 33 – 35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9 – 14, 17 – 23, and 33 – 35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/07/2006, 08/06/2008, 09/19/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is issued in response to applicant filed request for continued examination (RCE) on 08/06/2008.

2. Claims 9 – 10, 12 – 13, 17 – 20, 22 – 23, and 33 have been amended. Claims 34 – 35 were added. Claims 1 – 8, 15 – 16, and 24 – 32 were canceled.

3. Claims 9 – 14, 17 – 23, and 33 – 35 are pending in this application.

4. The information disclosure statement (IDS) was submitted on 11/07/2006, 08/06/2008, and 09/19/2008. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

5. The examiner makes note that the newly added limitations (see amendments to the claims dated 08/06/2008) recited in claim 33: "receiving a first credential from the user at a first said input device in communication with the local machine; receiving a second credential from the user at a second said input device in communication with the local machine; translating the first credential into the common credential protocol using a first one of the credential provider modules corresponding to the first input device that is in communication with the local machine; translating the second credential into the common credential protocol using a second one of the credential provider modules corresponding to the second input device that is in communication with the local machine; using a component of the OS to authenticate the translated first credential and second credential having the common credential protocol against a credential database; and logging the user on with the OS to access the local machine when the

authentication of both the first credential and the second credential is successful" do not contain proper amendment format since the limitations are not underlined.

6. Applicant's arguments with respect to newly added and amended claims 9 – 10, 12 – 13, 17 – 20, 22 – 23, and 33 – 35 have been considered but are moot in view of the new ground(s) of rejection.

Continued Examination Under 37 CFR 1.114

7. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/11/2006 has been entered.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 9 – 14, 17 – 23, and 33 – 35 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The limitations "enable" recited in claims 9, 13, 17, 22, 33, 34, 35; "capable of" recited in claims 9, 17, 22, 34, 35; "interoperable" recited in claims 13, 34; and "allowing" recited in claim 35 are indirect, passive, suggest optionally, which renders any recitation claimed after not be given patentable weight. Therefore, it is unclear what Applicant' intended metes and bounds of the claims are, since the claims appear to cover anything and everything that does not prohibit actions from occurring.

The Examiner points to MPEP 2106 [III-C] wherein the claim's recitation of "adapted to" raises the question to Language that suggests or makes optional but does not require steps to be performed or does not limit a claim to a particular structure does not limit the scope of a claim or claim limitation.

Office personnel must rely on the applicant's disclosure to properly determine the meaning of the terms "enable", "capable of", "interoperable", and "allowing" in the claims. Limitations appearing in the specification but not recited in the claim are not read into the claim; therefore, in this case, the recitation of "enable", "capable of", "interoperable", and "allowing" as interpreted in light of the specification provide the "functionality" or "the capability" of the system to perform the steps without definite disclosure limiting or excluding any alternative, negative, or even all together suggest actually performing or implementing the functionality that its database management system is capable of.

Therefore, any cited art that teaches the steps otherwise in the alternative can be used to reject the instant application. For example, the computer being enabled to perform a function does not mean that it will ever actually perform that functionality

(same reasoning applies to the terms: "capable of", "interoperable", and "allowing"). The terms "enable", "capable of", "interoperable", and "allowing" should be clarified and changed to a more definite terms.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

12. Claims 9 – 11, 13 – 14, 17 – 19, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Botz et al. (Botz hereinafter) (US Patent App. Pub. No.

2003/0177388 A1, filed: March 15, 2002) in view of Kao et al. (Kao hereinafter) (US Patent No. 6,651,168 B1, filed January 29, 1999).

Regarding Claim 9, Botz discloses a method comprising:

initializing, by a native operating system (OS) on a local machine, a logon user interface (UI) ([0060], [0084], Botz);

initializing, with the logon UI on the local machine, a plurality of different coexisting credential provider modules ([0010], **"between disparate security registry services which employ different forms** of user identification and authentication. In accordance with the authenticated identity translation technique disclosed herein, a caller of the service does not have to know which target system or systems a further request will be forwarded to in a multi-system environment. Further, using the present technique, user passwords exist only inside the protection offered by the security registry whereby a user initially authenticates, thereby facilitating administration of the system. Employing identity translation tokens in accordance with an aspect of the technique further provides trace delegation that encompasses multiple disparate security user registries. In addition, using a domain controller function to record identification and authentication events inside a domain enables management of a security state for a transaction in transit", Botz), each for translating respectively different types of credentials into a common credential protocol ([0008], "wherein the **translating includes employing a global registry of the different user identities** maintained by the domain controller to translate the authenticated user identity into the

local user identity **for the subsequent authentication** unit", Botz), the common credential protocol being, compatible with the native OS of the local machine ([0008], "wherein the **translating includes employing a global registry of the different user identities**", Botz), each said credential provider module enabling a user to log on with the native OS on the local machine via the logon UI to access the local machine ([0123] – [0125], Botz).

Botz also discloses a plurality of input devices (Fig. 13, items 1402, 1404, and 1400, Page 10, [0141], lines 3 – 5, Botz). However, Botz does not explicitly disclose different input devices. On the other hand, Kao discloses: using one of a plurality of corresponding different input devices that are capable of being in communication with the local machine (Fig. 1 A, items 222, 220, 210, 208, 212, and 224, Col. 8, lines 22 – 26 and 38 – 48, Kao). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Kao's teachings to the system of Botz. Skilled artisan would have been motivated to do so, as suggested by Kao (Col. 2, lines 25 – 28, Kao), to provide a flexible way to provide diverse user authentication mechanisms and processes for a stand alone computer system or for a computer network. In addition, both of the references (Botz and Kao) teach features that are directed to analogous art and they are directed to the same field of endeavor, such as, databases management systems, receiving credentials, and authentication. This close relation between both of the references highly suggests an expectation of success.

Furthermore, the combination of Botz in view of Kao (Botz/Kao hereinafter) discloses:

receiving a first said credential from the user at a first one of said input devices in communication with a the local machine (Page 1 and 2, [0007] and [0033], lines 11 –13, and 3 – 5 and 10 – 11, Botz[1]; and Fig. 1 A, items 222, 220, 210, 208, 212, and 224, Col. 8, lines 22 – 26 and 38 – 48, Kao);

translating the first credential with a first one of said credential provider modules corresponding to the first input device that is in communication with the local machine (Page 1, [0007], lines 13 – 17, Botz[2]; and Fig. 1, item 200, Col. 8, lines 22 – 26, "…The authentication framework 200 is designed to allow different kinds of authentication mechanisms to be plugged into the system…", Kao and also see Col. 9, lines 30 – 34; "The actual conversation function implementation converts these data attributes to determine the style or format ...", Kao);

communicating the translated first credential having the common credential protocol through a credential provider Application Program Interface (API) to the logon (UI) of the native OS, wherein the credential provider API is configured to interface with each of the plurality of different coexisting credential provider modules (Fig. 4, item 402, Page 5 and 6, [0071] and [0076], lines 1 – 4 and 1 – 5, the interfaces services; respectively, Botz; and Fig. 1, items 218, 214, 202, 203, Col. 7 and 8, lines 33 – 36 and 52 – 63; respectively, "In one application to the Global Sign-On (GSP) single sign-on client/server architecture, which is based on distributed computer environment (DCE)...retrieve information to a particular authentication process from a plugged in

[1] Wherein the step of forwarding implies the step of receiving the credential claimed. And wherein the user ID and password corresponds to the credential claimed.

authentication module such as the module 210, 208 and 212...for example a fingerprint scanner 224 or smart card 222...", Kao);

passing the translated first credential having the common credential protocol to an OS logon module of the native OS from the logon UI (Page 1, [0007], lines 13 – 17, Botz; and Col. 9, lines 24 – 27, Kao);

calling the OS logon module for the native OS to authenticate the translated credential having the common credential protocol against a credential database (Page 1, [0008], lines 6 – 9, Botz; and Col. 9, lines 24 – 27, Kao); and

logging the user on with the native OS to access the local machine when the authentication is successful (Page 3, [0034], lines 7 – 13, Botz[3]; and Col. 17, lines 23 – 26, Kao and also see Col. 9 – 10, lines 66 – 67 and 1 – 10, Kao).

Regarding Claim 10, Botz/Kao discloses a method, wherein the logging on of the user further comprises logging the user on to the local machine after one or more additional said credentials have been received, translated by a respective said different coexisting credential provider module, and authenticated successfully, in addition to said credential (Page 7, [0094], lines 6 – 10, wherein the identity of the initial authentication server, identity of the user, etc in [0099] - [0106] corresponds to the plurality of the credentials as claimed, Botz; and Col. 17, lines 23 – 26, Kao, Col. 9 – 10, lines 66 – 67 and 1 – 10, Kao, and also Col. 8, lines 64 – 67 , " a smart card 222 is

[2] Wherein the authenticated user identity corresponds to the credential (being translated) claimed; the initial authentication unit corresponds to one of different coexisting credential provider modules claimed; and the local user identity corresponds to the common credential protocol claimed.
[3] Wherein the step of sign-on corresponds to the step of logging the user claimed.

plugged into the smart card reader 220 and a user's DCE ID and password is stored in the smart card…", Kao).

Regarding Claim 11, Botz/Kao discloses a method, wherein the user is not logged on to the local machine at the time when the translated credentials are authenticated (Page 7, [0094], lines 6 – 10, Botz).

Regarding Claim 14, Botz/Kao discloses a computer-readable medium comprising instructions that, when executed by a computer (Page 2, [0030], lines 1 – 4, Botz).

Regarding Claim 17, Botz/Kao discloses a comprising:

Initializing, by a native operating system (OS) on a local machine, a logon user interface (UI) ([0060], [0084], Botz);

initializing, with the logon UI on the local machine, a plurality of different coexisting credential provider modules ([0010], "**between disparate security registry services which employ different forms** of user identification and authentication. In accordance with the authenticated identity translation technique disclosed herein, a caller of the service does not have to know which target system or systems a further request will be forwarded to in a multi-system environment. Further, using the present technique, user passwords exist only inside the protection offered by the security registry whereby a user initially authenticates, thereby facilitating administration of the

system. Employing identity translation tokens in accordance with an aspect of the technique further provides trace delegation that encompasses multiple disparate security user registries. In addition, using a domain controller function to record identification and authentication events inside a domain enables management of a security state for a transaction in transit", Botz), each said credential provider module configured to perform a translation of a respectively different type of credential received at a different type of input device in communication with the local machine for translating the respectively different types of credentials into a common credential protocol ([0008], "wherein the **translating includes employing a global registry of the different user identities** maintained by the domain controller to translate the authenticated user identity into the local user identity **for the subsequent authentication** unit", Botz), the common credential protocol being compatible with the native OS of the local machine ([0008], "wherein the **translating includes employing a global registry of the different user identities**", Botz), wherein each said credential provider module enables a user to log on with the native OS on the local machine via the logon UI to access the local machine using one of a plurality of corresponding different input devices that are capable of being in communication with the local machine ([0123] – [0125], Botz);

receiving a first credential from the user at a first one of said input devices in communication with the local machine (Page 1 and 2, [0007] and [0033], lines 11 –13,

and 3 – 5 and 10 – 11, Botz[4]; and Fig. 1 A, items 222, 220, 210, 208, 212, and 224, Col. 8, lines 22 – 26 and 38 – 48, Kao);

translating the first credential with a first one of said credential provider modules that corresponds to the first input device (Page 1, [0007], lines 13 – 17, Botz[5]; and Fig. 1, item 200, Col. 8, lines 22 – 26, "...The authentication framework 200 is designed to allow different kinds of authentication mechanisms to be plugged into the system...", Kao and also see Col. 9, lines 30 – 34; "The actual conversation function implementation converts these data attributes to determine the style or format ...", Kao);

communicating the translated first credential having the common credential protocol through a credential provider interface to the logon (UI) of the native OS, wherein the credential provider interface is configured to interface with each of the plurality of coexisting different said credential provider modules (Fig. 4, item 402, Page 5 and 6, [0071] and [0076], lines 1 – 4 and 1 – 5, the interfaces services; respectively, Botz; and Fig. 1, items 218, 214, 202, 203, Col. 7 and 8, lines 33 – 36 and 52 – 63; respectively, "In one application to the Global Sign-On (GSP) single sign-on client/server architecture, which is based on distributed computer environment (DCE)...retrieve information to a particular authentication process from a plugged in authentication module such as the module 210, 208 and 212...for example a fingerprint scanner 224 or smart card 222...", Kao);

---

[4] Wherein the step of forwarding implies the step of receiving the credential claimed. And wherein the user ID and password corresponds to the credential claimed.

[5] Wherein the authenticated user identity corresponds to the credential (being translated) claimed; the initial authentication unit corresponds to one of different coexisting credential provider modules claimed; and the local user identity corresponds to the common credential protocol claimed.

passing the translated first credential having the common credential protocol to a logon routine of the native OS from the logon UI (Page 1, [0007], lines 13 – 17, Botz; and Col. 9, lines 24 – 27, Kao);

authenticating the translated first credential against a credential database with the logon routine of the native OS (Page 3, [0034], lines 7 – 13, Botz[6]; and Col. 17, lines 23 – 26, Kao and also see Col. 9 – 10, lines 66 – 67 and 1 – 10, Kao); and

logging the user on to access the local machine with the native OS when the authentication is successful (Page 3, [0034], lines 7 – 13, Botz[7]; and Col. 17, lines 23 – 26, Kao and also see Col. 9 – 10, lines 66 – 67 and 1 – 10, Kao).

Regarding Claim 18, Botz/Kao discloses a method, wherein the logging on of the user to access the local machine with the native OS further comprises deferring the logging on of the user to access the local machined until the receiving, the translating, the communicating, the passing, and the authenticating successfully have been repeated for at least one more additional said credentials in addition to said first credential (Page 7, [0094], lines 6 – 10, Botz[8]).

Regarding Claim 19, Botz/Kao discloses a method, wherein the user is not logged on to access the local machine until after the translated credentials is

[6] Wherein the step of sign-on corresponds to the step of logging the user claimed.
[7] Wherein the step of sign-on corresponds to the step of logging the user claimed.
[8] Wherein the step of using the policy information, including trust policy and initial authentication, to signing the user on (Page 7, [0094], lines 1 – 6, Botz) corresponds to the step of logging the user claimed. In addition, Botz discloses the use of a plurality of credentials as claimed (Page 7, [0101], lines 3

authenticated against the credential database with the logon routine of the native OS (Page 7, [0094], lines 6 – 10, [0008], "wherein the translating includes employing a global registry of the different user identities maintained by the domain controller to translate the authenticated user identity into the local user identity for the subsequent authentication unit", Botz).

Regarding Claim 21, Botz/Kao discloses a computer-readable medium comprising instructions that, when executed by a computer, perform the method of claim 17 (Page 2, [0030], lines 1 – 4, Botz).

Regarding Claim 22, Botz/Kao discloses a computer-readable medium comprising a plurality of different coexisting credential provider modules initialized with a logon user interface (UI) by a native operating system (OS) on a local machine, each including instructions that, when executed by the local machine, receive and translate a credential into a common credential protocol so as to be compatible for authentication by an authentication component of the native OS against a credential database for logging a user identified by the credential on with the native OS to access the local machine when the authentication is successful, wherein:

the translated credential is received via a credential provider Application Programming Interface (API) of the authentication component of the native OS (Fig. 4, item 402, Page 5 and 6, [0071] and [0076], lines 1 – 4 and 1 – 5, the interfaces

– 14, Botz). By signing the user on after the information is authenticated, the system is deferring the

services; respectively, Botz; and Fig. 1, items 218, 214, 202, 203, Col. 7 and 8, lines 33 – 36 and 52 – 63; respectively, "In one application to the Global Sign-On (GSP) single sign-on client/server architecture, which is based on distributed computer environment (DCE)...retrieve information to a particular authentication process from a plugged in authentication module such as the module 210, 208 and 212...for example a fingerprint scanner 224 or smart card 222...", Kao);

the credential provider API (Fig. 3, items 314, and 316, Page 4, [0058], lines 1 – 4, Botz) of the authentication component of the native OS is compatible for receiving each of a plurality of said credentials (Page 1 and 2, [0007] and [0033], lines 11 – 13, and 3 – 5 and 10 – 13; respectively; wherein the step of forwarding implies the step of receiving the credential claimed. And wherein the user ID and password corresponds to the credential claimed; Botz) from a corresponding plurality of different coexisting credential provider modules (Page 1 and 4, [0007] and [0050], lines 13 – 17 and 1 – 6, multiple security user registries of multiple computer platforms; respectively, Botz; and Fig. 1, items 218, 214, 202, 203, Col. 7 and 8, lines 33 – 36 and 52 – 63; respectively, Kao); and

each said different coexisting credential provider module can:

receive a respective different type of said credential from a respective input device (Fig.10, items 1104, 1108, 1110, and 1112, Page 9, [0123], lines 8 – 11, Botz[9]), each respective input device capable of coupling to the local machine

signing on or logging on.

[9] Wherein examiner interprets the step where a first user signs on using Public Key infrastructure (PKI), and a second user signs on using Kerberos (Page 9, [0123], lines 8 – 11, Botz) as the step of receiving different type of credential from respective input device as claimed.

and enabling the user to log on with the native OS to access the local machine (Fig. 13, items 1402, 1404, and 1400, Page 10, [0141], lines 3 – 5, Botz; and Fig. 1 A, items 222, 220, 210, 208, 212, and 224, Col. 8, lines 22 – 26 and 38 – 48, Kao); and

translate each said different type of said credential into the credential protocol so as to be compatible for authentication by the authentication component of the native OS against the credential database (Page 3, [0039], lines 1 – 6, an infrastructure to support run-time cooperation between disparate security registry user, Botz; and Page 1, [0007], lines 13 – 17, Botz[10]; and Fig. 1, item 200, Col. 8, lines 22 – 26, "...The authentication framework 200 is designed to allow different kinds of authentication mechanisms to be plugged into the system...", Kao and also see Col. 9, lines 30 – 34; "The actual conversation function implementation converts these data attributes to determine the style or format ...", Kao).

Regarding Claim 33, Botz/Kao discloses a method comprising:

initializing, by a native operating system (OS) on a local machine, a logon user interface (UI) ([0060], [0084], Botz);

initializing, with the logon UI on the local machine, a plurality of different coexisting credential provider modules ([0010], "**between disparate security registry services which employ different forms** of user identification and authentication. In

accordance with the authenticated identity translation technique disclosed herein, a caller of the service does not have to know which target system or systems a further request will be forwarded to in a multi-system environment. Further, using the present technique, user passwords exist only inside the protection offered by the security registry whereby a user initially authenticates, thereby facilitating administration of the system. Employing identity translation tokens in accordance with an aspect of the technique further provides trace delegation that encompasses multiple disparate security user registries. In addition, using a domain controller function to record identification and authentication events inside a domain enables management of a security state for a transaction in transit", Botz), each said credential provider module configured to perform translation of a respectively different type of credential received at one of a plurality of different types of input devices in communication with the local machine for translating the respectively different types of credentials into a common credential protocol ([0008], "wherein the **translating includes employing a global registry of the different user identities** maintained by the domain controller to translate the authenticated user identity into the local user identity **for the subsequent authentication** unit", Botz), the common credential protocol being compatible with the native OS of the local machine ([0008], "wherein the **translating includes employing a global registry of the different user identities**", Botz), wherein each said credential provider module enables a user to log on with the native OS on the local machine via the logon UI to access the local machine ([0123] – [0125], Botz) using one of a plurality

[10] Wherein the authenticated user identity corresponds to the credential (being translated) claimed; the

of corresponding different input devices in communication with the local machine (Fig. 1 A, items 222, 220, 210, 208, 212, and 224, Col. 8, lines 22 – 26 and 38 – 48, Kao);

receiving a first credential from the user at a first said input device in communication with the local machine (Page 1 and 2, [0007] and [0033], lines 11 – 13, and 3 – 5 and 10 – 11; respectively, Botz[11]);

receiving a second credential from the user at a second said input device in communication with the local machine (Page 1 and 2, [0007] and [0033], lines 11 – 13, and 3 – 5 and 10 – 11; respectively, Botz[12]);

translating the first credential into the common credential protocol using a first one of the credential provider modules corresponding to the first input device that is in communication with the local machine (Page 1, [0007], lines 13 – 17, Botz[13]; and Fig. 1, item 200, Col. 8, lines 22 – 26, "…The authentication framework 200 is designed to allow different kinds of authentication mechanisms to be plugged into the system…", Kao and also see Col. 9, lines 30 – 34; "The actual conversation function implementation converts these data attributes to determine the style or format ...", Kao);

translating the second credential into the common credential protocol using a second one of the credential provider modules corresponding to the second input device that is in communication with the local machine (Page 1, [0007], lines 13 – 17,

---

initial authentication unit corresponds to one of different coexisting credential provider modules claimed; and the local user identity corresponds to the common credential protocol claimed.

[11] Wherein the step of forwarding implies the step of receiving the credential claimed. And wherein the user ID and password corresponds to the credential claimed.

[12] Wherein the step of forwarding implies the step of receiving the credential claimed. And wherein the user ID and password corresponds to the credential claimed.

[13] Wherein the authenticated user identity corresponds to the credential (being translated) claimed; the initial authentication unit corresponds to one of different coexisting credential provider modules claimed; and the local user identity corresponds to the common credential protocol claimed.

Botz[14]; and Fig. 1, item 200, Col. 8, lines 22 – 26, "...The authentication framework 200 is designed to allow different kinds of authentication mechanisms to be plugged into the system...", Kao and also see Col. 9, lines 30 – 34; "The actual conversation function implementation converts these data attributes to determine the style or format ...", Kao);

using a component of the OS to authenticate the translated first credential and second credential having the common credential protocol against a credential database (Fig. 13, items 1402, 1404, and 1400, Page 10, [0141], lines 3 – 5, Botz; and Fig. 1 A, items 222, 220, 210, 208, 212, and 224, Col. 8, lines 22 – 26 and 38 – 48, Kao); and

logging the user on with the OS to access the local machine when the authentication of both the first credential and the second credential is successful (Page 7, [0094], lines 6 – 10, wherein the identity of the initial authentication server, identity of the user, etc in [0099] - [0106] corresponds to the plurality of the credentials as claimed, Botz; and Col. 17, lines 23 – 26, Kao, Col. 9 – 10, lines 66 – 67 and 1 – 10, Kao, and also Col. 8, lines 64 – 67 , " a smart card 222 is plugged into the smart card reader 220 and a user's DCE ID and password is stored in the smart card...", Kao).

13. Claims 12, 20, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Botz et al. (Botz hereinafter) (US Patent App. Pub. No. 2003/0177388 A1, filed: March 15, 2002), in view of Kao et al. (Kao hereinafter) (US Patent No. 6,651,168 B1, filed January 29, 1999), and further in view of Axel et al.

[14] Wherein the authenticated user identity corresponds to the credential (being translated) claimed; the initial authentication unit corresponds to one of different coexisting credential provider modules claimed; and the local user identity corresponds to the common credential protocol claimed.

(Axel hereinafter) (US Patent App. Pub. No. 2004/0139355 A1, filed: November 7, 2002).

Regarding Claim 12, Botz/Kao discloses all the limitations as disclosed above including a method, wherein the use of the OS logon module of the native OS to authenticate the translated first credential having the common credential protocol against the credential database further comprises:

communicating the translated credential to an LSA (Page 7, [0090], lines 1 – 5, Botz[15]); and

determining the authentication with the LSA against the credential database (Page 7, [0090], lines 6 – 9, Botz[16]) that is selected from the group consisting of:

a local database other than the SAM database (Page 5, [0069], lines 3 – 5, local user registry, Botz);

a remote credential database (Page 5, [0067], lines 12 – 14, LDAP-accessible storage, Botz[17]);

a token protocol credential service (Page 9, [0133], lines 2 – 6, HyperText Transfer Protocol (HTTP), Botz);

---

[15] Wherein examiner interprets the AIT domain controller as the LSA claimed; and the identity translation token (ITT) and/or the identity translation token reference (ITTR) as the translated credential claimed.
[16] Wherein the step of validating the translated token using a copy of the signing value retained at the AIT domain controller corresponds to the step of determining the authentication against the credential database as claimed. In addition, Botz further discloses that this controller utilizes databases to store the information (Page 6, [0086], lines 3 – 7, Botz).
[17] Wherein the LDPA-accessible storage corresponds to the remote credential database claimed. The reason is because this storage is retrieved upon a server session, which would imply a remote session.

a challenge and response protocol service (Page 9, [0133], lines 1 – 6, HyperText Transfer Protocol (HTTP), Botz[18]);

In addition, Botz/Kao further discloses KDC (Fig. 10, item 1102, Kerberos, Botz). However, Botz/Kao does not expressly disclose a SAM database; and an AD at a domain remote from the local machine. On the other hand, Axel discloses a system including a SAM database (Page 2, [0018], lines 3 – 5, Axel); an AD (Page 2, [0017], lines 4 – 5, Axel) and KDC at a domain remote from the local machine (Page 2, [0017], lines 1 – 3, Axel); and an LSA (Page 2, [0021], lines 1 – 2, Axel). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Axel's teachings to the system Botz/Kao. Skilled artisan would have been motivated to do so, as suggested by Axel (Page 1, [0002], lines 1 – 4, Axel), to provide access to various password-enabled computer network elements through the use of a single password enabled network element.

Regarding Claim 20, the combination of Botz in view of Kao and further in view of Axel (Botz/Kao/Axel hereinafter) discloses a method, wherein the authenticating of the translated first credential against the credential database with the logon routine of the native OS further comprises:

communicating the translated credential to an LSA from the logon routine of the native OS (Page 7, [0090], lines 1 – 5, Botz[19]; and Page 2, [0021], lines 1 – 2, LSA, Axel); and

[18] Wherein the feature of extracting corresponds to the challenge claimed; and the feature of passing

determining the authentication with the LSA against the credential database (Page 7, [0090], lines 6 – 9, Botz[20]; and Page 2, [0021], lines 1 – 2, LSA, Axel) that is selected from the group consisting of:

a SAM database (Page 2, [0018], lines 3 – 5, Axel);

a local database other than the SAM database (Page 5, [0069], lines 3 – 5, local user registry, Botz);

a remote credential database (Page 5, [0067], lines 12 – 14, LDAP-accessible storage, Botz[21]);

a token protocol credential service (Page 9, [0133], lines 2 – 6, HyperText Transfer Protocol (HTTP), Botz);

a challenge and response protocol service (Page 9, [0133], lines 1 – 6, HyperText Transfer Protocol (HTTP), Botz[22]); and

an AD (Page 2, [0017], lines 4 – 5, Axel) and KDC at a domain remote from the local machine (Page 2, [0017], lines 1 – 3, Axel; and Fig. 10, item 1102, Kerberos, Botz).

---

corresponds to the response claimed.

[19] Wherein examiner interprets the AIT domain controller as the LSA claimed; and the identity translation token (ITT) and/or the identity translation token reference (ITTR) as the translated credential claimed.

[20] Wherein the step of validating the translated token using a copy of the signing value retained at the AIT domain controller corresponds to the step of determining the authentication against the credential database as claimed. In addition, Botz further discloses that this controller utilizes databases to store the information (Page 6, [0086], lines 3 – 7, Botz).

[21] Wherein the LDPA-accessible storage corresponds to the remote credential database claimed. The reason is because this storage is retrieved upon a server session, which implies a remote session.

[22] Wherein the feature of extracting corresponds to the challenge claimed; and the feature of passing corresponds to the response claimed.

Regarding Claim 23, Botz/Kao/Axel discloses a computer-readable medium, wherein the authentication component of the native OS comprises:

the logon (UI) (Page 6, [0076], lines 1 – 5, Botz; and Col. 8, lines 22 – 34, Kao);

an OS logon module for receiving Remote Procedure Call (RPC) calls from the logon UI module (Page 6, [0083], lines 1 – 5, remote sign-on, Botz; and Col. 8, lines 22 – 34, Kao); and

an LSA for determining the authentication, and in communication with, the credential database (Page 7, [0090], lines 6 – 9, Botz[23]) that is selected from the group consisting of:

a SAM database (Page 2, [0018], lines 3 – 5, Axel);

a local database other than the SAM database (Page 5, [0069], lines 3 – 5, local user registry, Botz);

a remote credential database (Page 5, [0067], lines 12 – 14, LDAP-accessible storage, Botz[24]);

a token protocol credential service (Page 9, [0133], lines 2 – 6, HyperText Transfer Protocol (HTTP), Botz);

a challenge and response protocol service (Page 9, [0133], lines 1 – 6, HyperText Transfer Protocol (HTTP), Botz[25]); and

---

[23] Wherein the step of validating the translated token using a copy of the signing value retained at the AIT domain controller corresponds to the step of determining the authentication against the credential database as claimed. In addition, Botz further discloses that this controller utilizes databases to store the information (Page 6, [0086], lines 3 – 7, Botz).

[24] Wherein the LDPA-accessible storage corresponds to the remote credential database claimed. The reason is because this storage is retrieved upon a server session, which implies a remote session.

[25] Wherein the feature of extracting corresponds to the challenge claimed; and the feature of passing corresponds to the response claimed.

an AD (Page 2, [0017], lines 4 – 5, Axel) and KDC at a domain remote from the local machine (Page 2, [0017], lines 1 – 3, Axel; and Fig. 10, item 1102, Kerberos, Botz).

14. Claims 13, 34 – 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Botz et al. (Botz hereinafter) (US Patent App. Pub. No. 2003/0177388 A1, filed: March 15, 2002), in view of Kao et al. (Kao hereinafter) (US Patent No. 6,651,168 B1, filed January 29, 1999), and further in view of Wen et al. (Wen hereinafter) (US 2003/0046392).

Regarding Claim 13, Botz/Kao discloses all the limitations as disclosed above. However, Botz/Kao does not expressly disclose: initializing one or more pre-logon access provider (PLAP) modules at the local machine coexisting. On the other hand, Wen discloses: initializing one or more pre-logon access provider (PLAP) modules at the local machine coexisting, with said credential provider modules, each PLAP module being interoperable with the OS of the local machine for enabling the user to select a logon connection type out of a plurality of logon connection types for establishing a network connection (Fig. 3A, and 3B, [0032], Wen). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the Wenl's teachings to the system Botz/Kao. Skilled artisan would have been motivated to do so, as suggested by Wen ([0011], Wen), to provide a network connecting system and

method that has an intuitive correspondence with the experience in real life to facilitate the network-connecting operation.

Furthermore, the combination of Botz in view of Kao and further in view of Wen (Botz/Kao/Wen hereinafter) discloses:

establishing by a selected one of said one or more PLAP modules a network connection from the local machine to a domain using the translated first credential (Page 1, [0007], lines 13 – 17, Botz[26]; Fig. 1, item 200, Col. 8, lines 22 – 26, "…The authentication framework 200 is designed to allow different kinds of authentication mechanisms to be plugged into the system…", Col. 9, lines 30 – 34; "The actual conversation function implementation converts these data attributes to determine the style or format ...", Kao; and Fig. 3A, and 3B, [0032], Wen).

Regarding Claim 34, Botz/Kao/Wen discloses a method comprising:

initializing, by a native operating system (OS) on a local machine, a logon user interface (UI) ([0060], [0084], Botz);

initializing with the logon UI on the local machine a plurality of different coexisting credential provider modules ([0010], **"between disparate security registry services which employ different forms** of user identification and authentication. In accordance with the authenticated identity translation technique disclosed herein, a caller of the service does not have to know which target system or systems a further request will be forwarded to in a multi-system environment. Further, using the present technique, user

passwords exist only inside the protection offered by the security registry whereby a user initially authenticates, thereby facilitating administration of the system. Employing identity translation tokens in accordance with an aspect of the technique further provides trace delegation that encompasses multiple disparate security user registries. In addition, using a domain controller function to record identification and authentication events inside a domain enables management of a security state for a transaction in transit", Botz), each for translating respectively different types of credentials into a common credential protocol ([0008], "wherein the **translating includes employing a global registry of the different user identities** maintained by the domain controller to translate the authenticated user identity into the local user identity **for the subsequent authentication** unit", Botz), the common credential protocol being, compatible with the native OS of the local machine ([0008], "wherein the **translating includes employing a global registry of the different user identities**", Botz), each said credential provider module enabling a user to log on with the native OS on the local machine via the logon UI to access the local machine ([0123] – [0125], Botz), using one of a plurality of corresponding different input devices that are capable of being in communication with the local machine (Fig. 13, items 1402, 1404, and 1400, Page 10, [0141], lines 3 – 5, Botz; and Fig. 1 A, items 222, 220, 210, 208, 212, and 224, Col. 8, lines 22 – 26 and 38 – 48, Kao);

initializing one or more pre-logon access provider (PLAP) modules at the local machine coexisting with said credential provider modules, each PLAP module being

[26] Wherein the authenticated user identity corresponds to the credential (being translated) claimed; the

interoperable with the OS of the local machine for enabling the user to select a logon connection type out of a plurality of logon connection types for establishing a network connection (Fig. 3A, and 3B, [0032], Wen);

receiving a first said credential from the user at a first one of said input devices in communication with the local machine (Page 1 and 2, [0007] and [0033], lines 11 –13, and 3 – 5 and 10 – 11, Botz[27]; and Fig. 1 A, items 222, 220, 210, 208, 212, and 224, Col. 8, lines 22 – 26 and 38 – 48, Kao);

translating the first credential with a first one of said credential provider modules corresponding to the first input device that is in communication with the local machine (Page 1, [0007], lines 13 – 17, Botz[28]; and Fig. 1, item 200, Col. 8, lines 22 – 26, "...The authentication framework 200 is designed to allow different kinds of authentication mechanisms to be plugged into the system...", Kao and also see Col. 9, lines 30 – 34; "The actual conversation function implementation converts these data attributes to determine the style or format ...", Kao);

establishing by a selected one of said PLAP modules a network connection from the local machine to a domain using the translated first credential (Page 1, [0007], lines 13 – 17, Botz[29]; Fig. 1, item 200, Col. 8, lines 22 – 26, "...The authentication framework 200 is designed to allow different kinds of authentication mechanisms to be plugged into

---

initial authentication unit corresponds to one of different coexisting credential provider modules claimed; and the local user identity corresponds to the common credential protocol claimed.

[27] Wherein the step of forwarding implies the step of receiving the credential claimed. And wherein the user ID and password corresponds to the credential claimed.

[28] Wherein the authenticated user identity corresponds to the credential (being translated) claimed; the initial authentication unit corresponds to one of different coexisting credential provider modules claimed; and the local user identity corresponds to the common credential protocol claimed.

the system…", Col. 9, lines 30 – 34; "The actual conversation function implementation converts these data attributes to determine the style or format ...", Kao; and Fig. 3A, and 3B, [0032], Wen);

communicating the translated first credential having the common credential protocol through a credential provider interface to the logon UI of the native OS, wherein the credential provider interface is configured to interface with each of the plurality of coexisting different said credential provider modules (Fig. 4, item 402, Page 5 and 6, [0071] and [0076], lines 1 – 4 and 1 – 5, the interfaces services; respectively, Botz; and Fig. 1, items 218, 214, 202, 203, Col. 7 and 8, lines 33 – 36 and 52 – 63; respectively, "In one application to the Global Sign-On (GSP) single sign-on client/server architecture, which is based on distributed computer environment (DCE)...retrieve information to a particular authentication process from a plugged in authentication module such as the module 210, 208 and 212...for example a fingerprint scanner 224 or smart card 222...", Kao);

passing the translated first credential having the common credential protocol to a logon routine of the native OS from the logon UI (Page 1, [0007], lines 13 – 17, Botz; and Col. 9, lines 24 – 27, Kao);

authenticating the translated first credential against a credential database with the logon routine of the native OS (Page 1, [0008], lines 6 – 9, Botz; and Col. 9, lines 24 – 27, Kao); and

---

[29] Wherein the authenticated user identity corresponds to the credential (being translated) claimed; the initial authentication unit corresponds to one of different coexisting credential provider modules claimed; and the local user identity corresponds to the common credential protocol claimed.

logging the user on to access the local machine with the native OS when the authentication is successful (Page 3, [0034], lines 7 – 13, Botz[30]; and Col. 17, lines 23 – 26, Kao and also see Col. 9 – 10, lines 66 – 67 and 1 – 10, Kao).

Regarding Claim 35, Botz/Kao/Wen discloses a method comprising:

initializing, by a native operating system (OS) on a local machine, a logon user interface (UI) ([0060], [0084], Botz);

initializing, with the logon UI on the local machine, a plurality of different coexisting credential provider modules ([0010], "**between disparate security registry services which employ different forms** of user identification and authentication. In accordance with the authenticated identity translation technique disclosed herein, a caller of the service does not have to know which target system or systems a further request will be forwarded to in a multi-system environment. Further, using the present technique, user passwords exist only inside the protection offered by the security registry whereby a user initially authenticates, thereby facilitating administration of the system. Employing identity translation tokens in accordance with an aspect of the technique further provides trace delegation that encompasses multiple disparate security user registries. In addition, using a domain controller function to record identification and authentication events inside a domain enables management of a security state for a transaction in transit", Botz), each said credential provider module configured to perform a translation of a respectively different type of credential received

[30] Wherein the step of sign-on corresponds to the step of logging the user claimed.

at a different type of input device in communication with the local machine for translating the respectively different types of credentials into a common credential protocol ([0008], "wherein the **translating includes employing a global registry of the different user identities** maintained by the domain controller to translate the authenticated user identity into the local user identity **for the subsequent authentication** unit", Botz), the common credential protocol being compatible with the native OS of the local machine ([0008], "wherein the **translating includes employing a global registry of the different user identities**", Botz), wherein each said credential provider module enables a user to log on with the native OS on the local machine via the logon UI to access the local machine ([0123] – [0125], Botz) using one of a plurality of corresponding different input devices that are capable of being in communication with the local machine (Fig. 1 A, items 222, 220, 210, 208, 212, and 224, Col. 8, lines 22 – 26 and 38 – 48, Kao);

receiving a credential from a user at an input device in communication with a local machine having a OS (Page 1 and 2, [0007] and [0033], lines 11 – 13, and 3 – 5 and 10 – 11; respectively, Botz[31]), the local machine capable of being in communication with a plurality of different input devices each configured to enable the user to log on with the OS to access local machine (Fig. 13, items 1402, 1404, and 1400, Page 10, [0141], lines 3 – 5, Botz; and Fig. 1 A, items 222, 220, 210, 208, 212, and 224, Col. 8, lines 22 – 26 and 38 – 48, Kao);

allowing a user to choose one of said plurality of different types of input devices to be used for logging on (Fig. 3A, and 3B, [0032], Wen);

receiving a first credential from the user via a selected first one of said input devices in communication with the local machine (Page 1 and 2, [0007] and [0033], lines 11 –13, and 3 – 5 and 10 – 11, Botz[32]; and Fig. 1 A, items 222, 220, 210, 208, 212, and 224, Col. 8, lines 22 – 26 and 38 – 48, Kao);

translating the first credential with a first one of said credential provider modules that corresponds to the first input device (Page 1, [0007], lines 13 – 17, Botz[33]; and Fig. 1, item 200, Col. 8, lines 22 – 26, "…The authentication framework 200 is designed to allow different kinds of authentication mechanisms to be plugged into the system…", Kao and also see Col. 9, lines 30 – 34; "The actual conversation function implementation converts these data attributes to determine the style or format ...", Kao);

communicating the translated first credential having the common credential protocol through a credential provider interface to the logon UI of the native OS, wherein the credential provider interface is configured to interface with each of the plurality of coexisting different said credential provider modules (Fig. 4, item 402, Page 5 and 6, [0071] and [0076], lines 1 – 4 and 1 – 5, the interfaces services; respectively, Botz; and Fig. 1, items 218, 214, 202, 203, Col. 7 and 8, lines 33 – 36 and 52 – 63; respectively, "In one application to the Global Sign-On (GSP) single sign-on client/server architecture, which is based on distributed computer environment (DCE)...retrieve information to a particular authentication process from a plugged in

[31] Wherein the step of forwarding implies the step of receiving the credential claimed. And wherein the user ID and password corresponds to the credential claimed.
[32] Wherein the step of forwarding implies the step of receiving the credential claimed. And wherein the user ID and password corresponds to the credential claimed.

authentication module such as the module 210, 208 and 212...for example a fingerprint scanner 224 or smart card 222...", Kao);

passing the translated first credential having the common credential protocol to a logon routine of the native OS from the logon UI (Page 1, [0007], lines 13 – 17, Botz; and Col. 9, lines 24 – 27, Kao);

authenticating the translated first credential against a credential database with the logon routine of the native OS (Page 1, [0008], lines 6 – 9, Botz; and Col. 9, lines 24 – 27, Kao); and

logging the user on to access the local machine with the native OS when the authentication is successful (Page 3, [0034], lines 7 – 13, Botz[34]; and Col. 17, lines 23 – 26, Kao and also see Col. 9 – 10, lines 66 – 67 and 1 – 10, Kao).

Response to Arguments

15. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

---

[33] Wherein the authenticated user identity corresponds to the credential (being translated) claimed; the initial authentication unit corresponds to one of different coexisting credential provider modules claimed; and the local user identity corresponds to the common credential protocol claimed.
[34] Wherein the step of sign-on corresponds to the step of logging the user claimed.

16. Applicant argues that; "Kao fails to teach or suggest initializing, with the logon UI on the local machine, a plurality of different coexisting credential provider modules, each for translating respectively different types of credentials into a common credential protocol, the common credential protocol being, compatible with the native OS of the local machine".

Applicant respectfully disagrees. The applied art does disclose: initializing, with the logon UI on the local machine, a plurality of different coexisting credential provider modules ([0010], "**between disparate security registry services which employ different forms** of user identification and authentication. In accordance with the authenticated identity translation technique disclosed herein, a caller of the service does not have to know which target system or systems a further request will be forwarded to in a multi-system environment. Further, using the present technique, user passwords exist only inside the protection offered by the security registry whereby a user initially authenticates, thereby facilitating administration of the system. Employing identity translation tokens in accordance with an aspect of the technique further provides trace delegation that encompasses multiple disparate security user registries. In addition, using a domain controller function to record identification and authentication events inside a domain enables management of a security state for a transaction in transit", Botz), each for translating respectively different types of credentials into a common credential protocol ([0008], "wherein the **translating includes employing a global registry of the different user identities** maintained by the domain controller to

translate the authenticated user identity into the local user identity **for the subsequent authentication** unit", Botz), the common credential protocol being, compatible with the native OS of the local machine ([0008], "wherein the **translating includes employing a global registry of the different user identities**", Botz). Additionally, the examiner notes that the step of "each for translating..." is a recitation of intended use. Wherein the recitation "for translating..." suggests or makes optional but does not require steps to be performed. A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

According to MPEP 2106; "The subject matter of a properly construed claim is defined by the terms that limit its scope. It is this subject matter that must be examined. As a general matter, the grammar and intended meaning of terms used in a claim will dictate whether the language limits the claim scope. Language that suggests or makes optional but does not require steps to be performed or does not limit a claim to a particular structure does not limit the scope of a claim or claim limitation. The following are examples of language that may raise a question as to the limiting effect of the language in a claim:

(A) statements of intended use or field of use,

(B) "adapted to" or "adapted for" clauses,

(C) "wherein" clauses, or

(D) "whereby" clauses."

17. Applicant argues that the applied art fails to disclose; "using a first credential translated by a first credential provider module and a second credential translated by a second credential provider module, that includes logging the user on with an OS on a local machine when the authentication of both the first credential and the second credential is successful".

Applicant respectfully disagrees. The applied art does disclose such newly added limitations (see rejection of claim 33 discussed in this Office Action above).

18. Applicant argues that; "Kao does not teach a first credential translated by a first credential provider module and a second credential translated by a second credential provider module".

Applicant respectfully disagrees. The applied art does disclose such newly added limitations (see rejection of claim 33 discussed in this Office Action above).

Points Of Contact

Any inquiry concerning this communication or earlier communications from the examiner should be directed to GIOVANNA COLAN whose telephone number is (571)272-2752. The examiner can normally be reached on 8:30 am - 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Breene can be reached on (571) 272-4107. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Giovanna Colan
Examiner
Art Unit 2162
October 08, 2008

/Jean M Corrielus/
Primary Examiner, Art Unit 2162